IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124163

Integrated Security Framework for Healthcare Using Fog Computing

Priyadharshini S[1], Pushparoja S[2], Pratheeba R[3], Chandralekha P[4]

Student, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[1]

Student, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[2]

Assistant Professor, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India [3]

Assistant Professor, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[4]

Abstract: Recent advancements in remote healthcare systems have attracted the attention of the IT industry, which can now offer solutions that are both widely used and simple to set up. Using computer resources as a service provided via the internet on demand is known as cloud computing. These systems provide a platform for the fully automated and ubiquitous exchange of medical knowledge, data, applications, and underpinning. Privacy and communication security would increase users' trust in such remote healthcare solutions. This study describes a cloud-based infrastructure for safe data for the healthcare industry. The research effort reported here is broken down into two categories: first, it attempts to protect key generation based on SHA algorithms, and second, it ensures patient privacy by securely maintaining electronic medical records (EMRs) in a hospital or clinical community cloud. According to the assessment and study, Hybrid Security approaches provide considerable security measures due to their very effective key generation process. It builds a private cloud where private patient data can be kept. Healthcare firms adopting public cloud services also gain from scalability. By eliminating both active and passive threats from the cloud network environment, these outcomes lead to the achievement of data confidentiality, data integrity, authentication, and authorization. The original data in this module is encrypted into two distinct values. Before being stored on the cloud, the data in each slice can be encrypted using various cryptographic algorithms and an encryption key.

Keywords: Healthcare, Fog Computing, Security, Framework, Advanced Encryption Standard (AES), Data Encryption Standard (DES), Secure Hash Algorithm (SHA), Encryption, Decryption, Convergent, Privilege.

I INTRODUCTION

Users face a severe strain storing the vast amount of data locally due to the data explosion. As a result, more and more businesses and people want to keep their data in the cloud. Unfortunately, the inevitable software problems, hardware issues, and human errors in the cloud could cause the data to be lost or destroyed. Several remote data integrity auditing systems have been put out to determine whether the data is stored appropriately in the cloud.Data blocks must first be signed by the data owner before being sent to the cloud in remote data integrity auditing methods. In the phase of integrity audits, these signatures are employed to demonstrate that the cloud actually contains these data blocks.

The data owner then uploads these data blocks and their associated signatures to the cloud. In several cloud storage services, like Google Drive, Dropbox, and iCloud, the data is frequently shared among many users.One of the most popular aspects of cloud storage is data sharing, which enables many users to share their data with others. Nonetheless, certain sensitive information may be included in these shared data storage locations in the cloud. For instance, confidential patient information (patient name, phone number, and ID number, etc.) and sensitive hospital information (hospital name, etc.) are typically maintained and exchanged in electronic health records. The researchers and the cloud will unavoidably come into contact with sensitive patient and hospital data if these EHRs are directly transferred to the cloud for research reasons.In addition, the EHRs' integrity must be ensured due to the possibility of human mistake and software/hardware malfunctions on the cloud. A possible solution to this issue is to encrypt the entire shared file before uploading it to the cloud, create the signatures needed to confirm the authenticity of the encrypted file, and then upload the encrypted file together with its matching signatures. Due to the fact that only the data owner is able to decode this file, this strategy can effectively hide important.But it will prevent others from using the entire shared file. For instance, encrypting the electronic health records (EHRs) of patients with contagious diseases can safeguard both patient and hospital privacy, but these encrypted EHRs are no longer useful to researchers.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.124163

The foregoing issue might be resolved by giving the researchers access to the decryption key.Unfortunately, for the reasons listed below, using this approach in actual situations is impractical. First of all, distributing a decryption key requires safe means, which can be challenging in particular situations. Furthermore, when a user uploads their EHRs to the cloud, it appears to be exceedingly difficult to predict which researchers would use them in the near future. As a result, encrypting the entire shared file is impractical for hiding important information. So, it is crucial and helpful to understand how to implement data sharing with sensitive information concealed in remote data integrity audits. Regrettably, this issue has not been investigated in earlier studies.

II LITERATURE REVIEW

1. By Yousaf et al. (2019), "Fog-Based Security and Privacy Framework for Healthcare Applications": The security and privacy framework for healthcare applications that is proposed in this study includes data encryption, authentication, and access control. The framework is created to handle the security and privacy issues that patients and healthcare professionals must deal with.

2. Amin et al.'s "Fog Computing-Based Healthcare Monitoring System: A Review" (2020): With an emphasis on security and privacy concerns, this study reviews healthcare monitoring systems based on fog computing. The authors talk about access control, intrusion detection, and encryption as methods for protecting healthcare data in fog computing environments.

3. Choudhary et al.'s "Secure Healthcare Data Transmission in Fog Computing" (2020): In this paper, a framework for safe healthcare data transmission in fog computing settings is proposed. To protect the confidentiality and integrity of healthcare data, the framework combines encryption, authentication, and access control.

4. Khalid et al.'s "Fog Computing for Healthcare: A Review" (2020): The application of fog computing in healthcare is thoroughly reviewed in this research, with an emphasis on security and privacy concerns. The authors go over various architectures for fog computing as well as security measures that can be utilised to protect medical data in these environments.

5. Zhang et al. (2018)'s "A Fog Computing-Based Security Framework for Healthcare" This study suggests a security framework for healthcare that uses fog computing and includes data encryption, access control, and intrusion detection. The framework is made to address the security and privacy issues that patients and healthcare professionals encounter in environments with fog computing.

6. By Li et al. (2021), "Fog Computing-Based Security Framework for IoT-Enabled Healthcare Systems": In this research, a security framework for IoT- enabled healthcare systems is proposed. This framework consists of data encryption, access control, and intrusion detection. The framework's goal is to deliver dependable and safe healthcare services in environments with fog computing.

7. By Xie et al. (2020), "A Secure and Scalable Fog Computing-Based Framework for Healthcare": In this research, a fog computing-based security and scalability framework for healthcare is proposed. This framework comprises data encryption, access control, and intrusion detection. The framework is intended to provide great scalability and dependability in addition to addressing the security and privacy problems faced by healthcare practitioners and patients in fog computing environments.

III EXISTING SYSTEM

The most important factor is that any person and every organisation can use cloud storage. From big to small, in groups or alone, the use of grid infrastructure can be put to best use for performance. As a result, Stone Soft has identified 5 techniques that IT departments can take to safeguard themselves from attacks and risks related to cloud security while maintaining the efficacy of their cloud computing initiatives.

The focus of the present systems is on preserving the integrity of the data and archiving it, but the problem of secrecy still exists and hasn't been totally resolved. Each of these systems lacks security assurance, making it impossible for consumers to have faith in their security.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

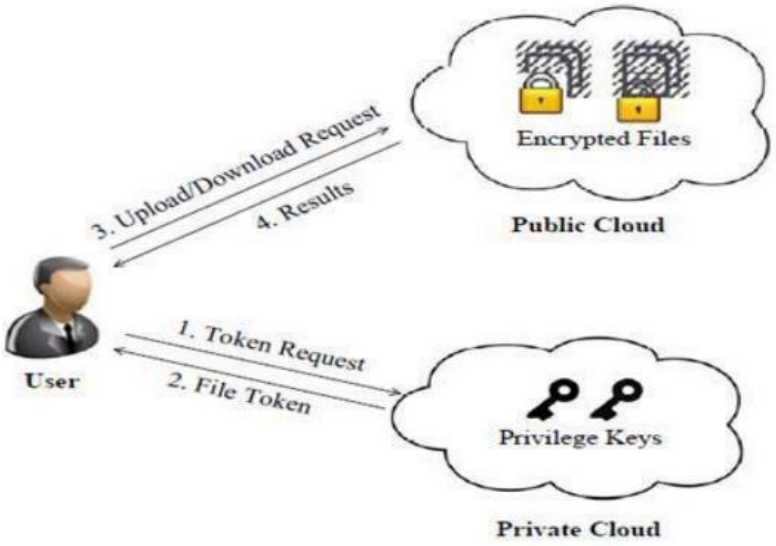
DOI: 10.17148/IJARCCE.2023.124163

IV PROPOSED SYSTEM

Users can store their data using cloud computing. The amount of data kept in the cloud is sufficient. Yet, security is a problem that restricts cloud computing's application; therefore, cloud computing hastens the development of security solutions. Everyone uses the cloud to store their data since it is simple and easy to utilize. Data availability, security, privacy, and dependability are the responsibility of the cloud service provider (CSP). Yet, because the CSP has complete control over the data after it is uploaded to the cloud and the user does not, the CSP does not offer the user total protection. Any action could be taken by the CSP with the user's data.

This lack of data control causes more serious security problems. This paper discusses using the public cloud to store data securely and protect it from illegal access. Cryptographic technology is employed to determine a person's authenticity. Security both inside and outside is therefore removed. As a result, cloud-based exercises for data protection, media trustworthiness, validation, and copyright are completed. Provide a reliable framework that can execute and store reliable administrations at all public cloud usage levels. Using the SHA (Secure Hashing algorithm) algorithm increases data security.

V SYSTEM ARCHITECTURE



The system model for the data exchange scheme and associated security model are provided in this section. Three distinct parties make up the data sharing system: the cloud server, the data owner, and the data sharer. In order to protect data owner privacy and the security of cloud data that has been outsourced, this study suggests a safe data exchange method. By addressing the privacy and security concerns for data sharing, the suggested approach offers flexible data utility. The developed scheme is practical and effective, as shown by the security and efficiency analyses. Finally, we talk about how it can be used in an electronic health record.

Data Owner: A data owner is a company whose enormous amounts of data will be processed and stored on cloud servers. Either the patients or the hospital are to blame.

Data Sharer: A person or organisation that will distribute the remote data of the data owners. It might be a medical or health researcher, a medical or health research organisation,

Cloud Server: A cloud service provider is the organisation that controls a cloud server. It has a sizable amount of storage space and computing power that it uses to process the data belonging to the data owners.

VI IMPLEMENTATION

Data Users: A user is an organisation that wants to contract with a storage cloud service provider (S-CSP) to store data and then access it later. To conserve upload bandwidth in a storage system that supports deduplication, a user only uploads unique data—which may belong to the same user or to different users—and does not upload any duplicate data.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023
DOI: 10.17148/IJARCCE.2023.124163

Private Cloud: This organisation helps consumers use cloud services in a secure manner. Users receive the file token from private cloud, which also manages the private keys for rights. In particular, private cloud is able to provide data user/owner with an execution environment and infrastructure acting as an interface between user and the public cloud because computing resources at data user/owner side are constrained and the public cloud is not fully trusted in practice.

S-CSP (storage cloud service provider): This is a company that offers a public cloud data storage service. On behalf of users, the SCSP offers a data outsourcing service and stores data. The SCSP uses deduplication to remove redundant data from storage and retains only unique data in order to lower storage costs. In this study, we assume that S-CSP has a lot of storage and processing power and is always online.

An open cloud is used to execute the complete model. The Openshift public cloud is used in this model of the cloud environment. For coding, JDK 1.6 and NetBeans are used. These are some important snapshots.

Encryption: Using file decryption and encryption, this form completes the model's first stage, which is the creation of private and public keys. The Data Owner just uploads their file and its public key using this method. The public key serves as the owner's identify on the cloud server. The private key is returned by this form after encrypting the files.

File Upload: There are steps involved in the file upload technique. The Clair text is first encrypted using the AES technique. At the second stage, encrypt the AES key using the SHA method. This function is used by the algorithm: Block number (F): The return value is the total number of blocks in file F. ENC AES (B, K): Block B is encrypted using the AES algorithm and the K key. Transmit to cloud (F'): This command allows you to upload the encrypted file F to cloud storage.

It makes it possible to upload the encrypted file F to cloud storage. ENC SHA (k): K is encrypted using the SHA algorithm. K' can be saved on the server using this feature.

Algorithm: File Upload

1. Encrypt file (F) {
2. /* a method for encrypting files and storing them in the cloud */
3. /* to convert Clair text from file F to Cipher text from file F */
4. /* Phase 1: Use the AES technique to encrypt Clair's text. */
5. For B ← 1 to number of block (F) do
6. 6. {
7. B=ENC AES (B, K)
8. }
9. Convey to cloud (F)
10. /* Phase 2: Encrypt AES Key with SHA algorithm */
11. For k ← 1 to size of (K) do P9
12. {
13. K= ENC SHA (K)
14. }
15. Save in server (K)
16. }
17. Convey to cloud (F)
18. /* Phase 2: Encrypt AES Key with SHA algorithm */
19. For k ← 1 to size of (K) do P9

Decryption: With the private key, this method decrypts the file. A list of the access rights for authenticated users is also necessary for this form.

Downloading a file: Moreover, this strategy is split into two halves. The AES key is first decrypted using the SHA Algorithm in the algorithm. The AES key obtained from the server in the second phase is then used to translate the encrypted text. The algorithm employs the following operations: Block number (F): The return value is the total number of blocks in file F. DEC SHA (k'): K' is decrypted using the SHA algorithm. DEC AES (B', K): Block B' is decrypted using the AES technique and key K.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124163

Algorithm: File Download

```
1.  Decrypt file (F) {
2.  /* decryption algorithm for files downloaded via cloud storage */
3.  /* to convert Cipher text contained in file F to Clair text contained in file F */
4.   /* Phase 1; AES key decryption using the SHA technique */
5.   for K ← 1 to size of (K) do
6.   6. {
7. K= DEC SHA (k) 8.}
9.  return (K)
10.   /* Phase: 2 AES algorithm is used to decrypt cypher text */
11.  for B ← 1 is the number of block (F) do
12. {
13. B= DEC AES (B, K)
14.}
 15. return (F)
  16}
```

VII RESULT AND DISCUSSION

We test our prototype and evaluate it depending on the results. Our study focuses on contrasting the convergent encryption and file upload processes with the overhead caused by authorization steps, such as file token generation and sharing token generation. We assess the overhead by adjusting several criteria.

VIII OUTPUT

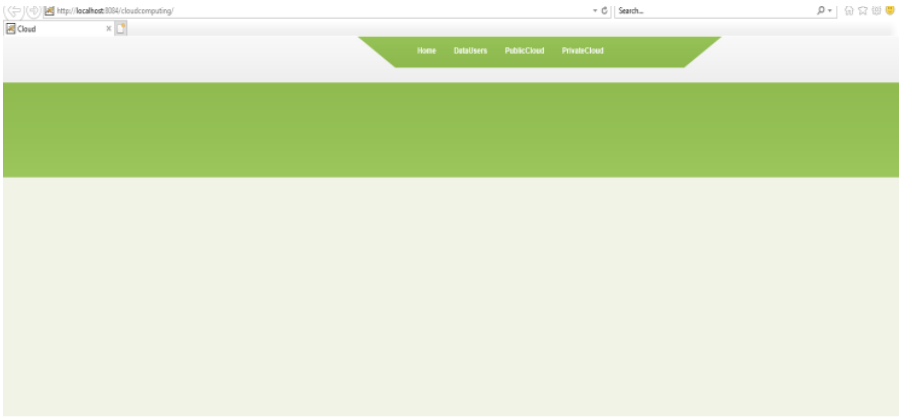


Figure 8.1Home Page

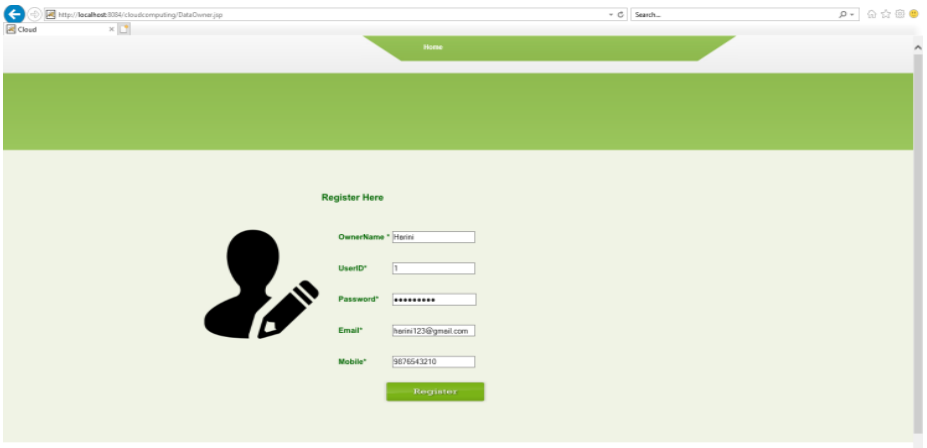


Figure 8.2 registration page

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124163

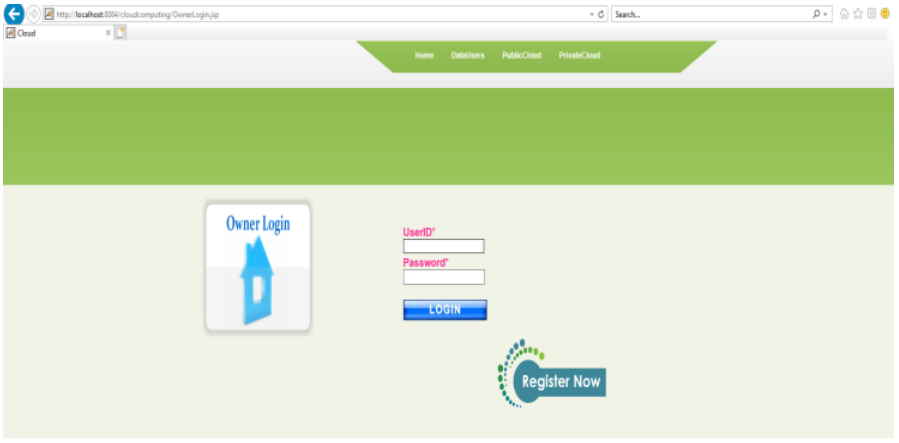


Figure 8.3 Login page

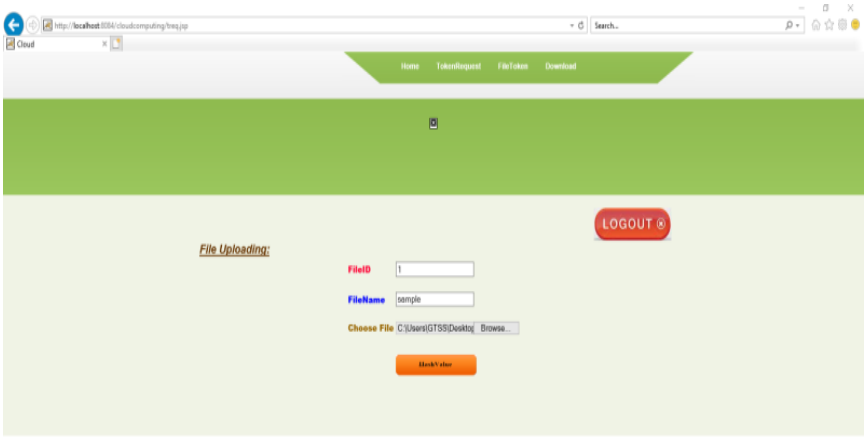


Figure 8.4 File upload

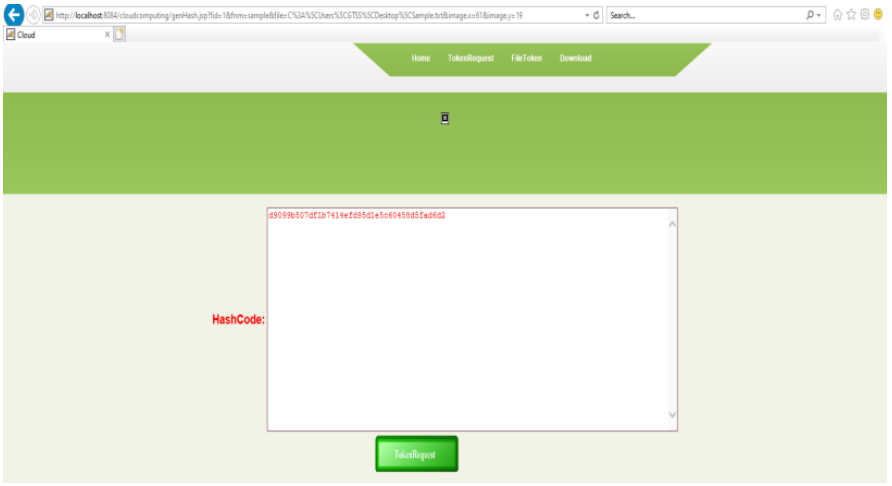


Figure 8.5 Token generation

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124163

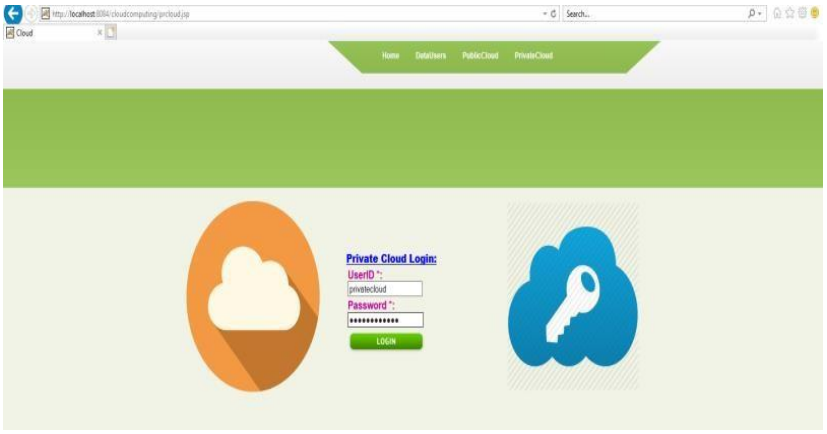


Figure 8.6 Private cloud login

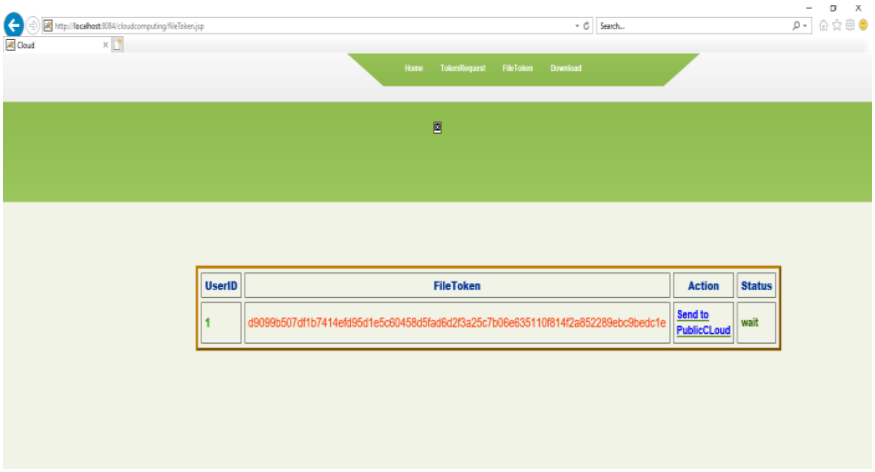


Figure 8.7 File token

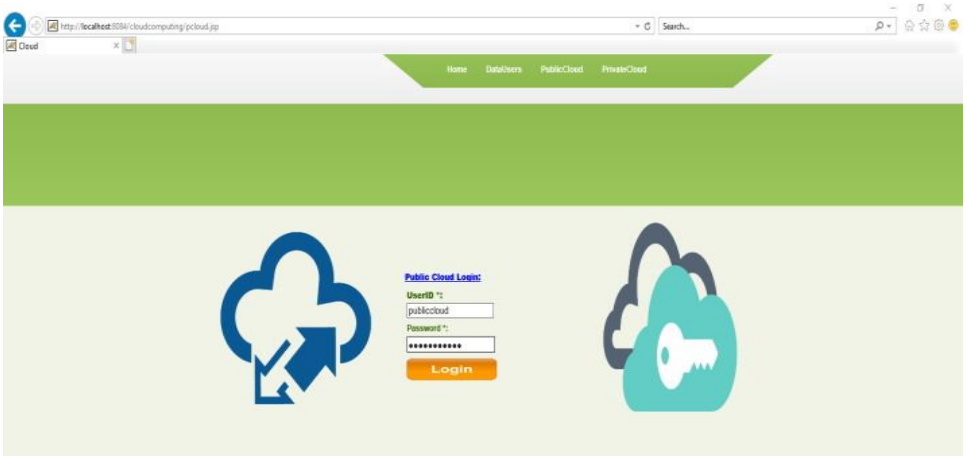


Figure 8.8 Public cloud login

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124163

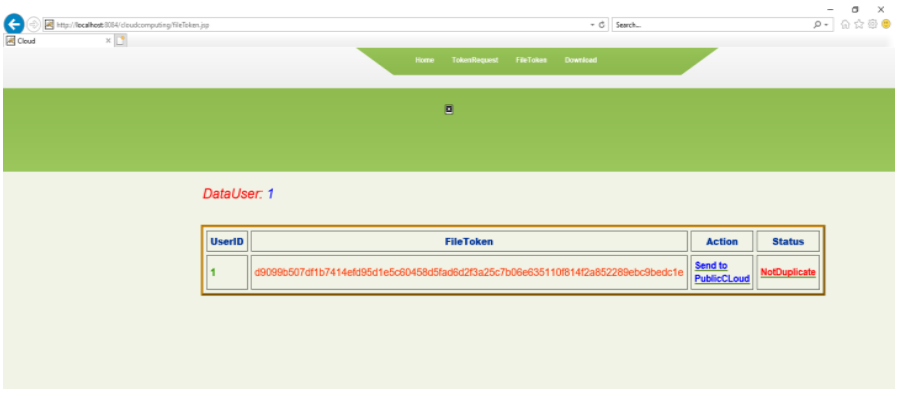


Figure 8.9 File duplicate check

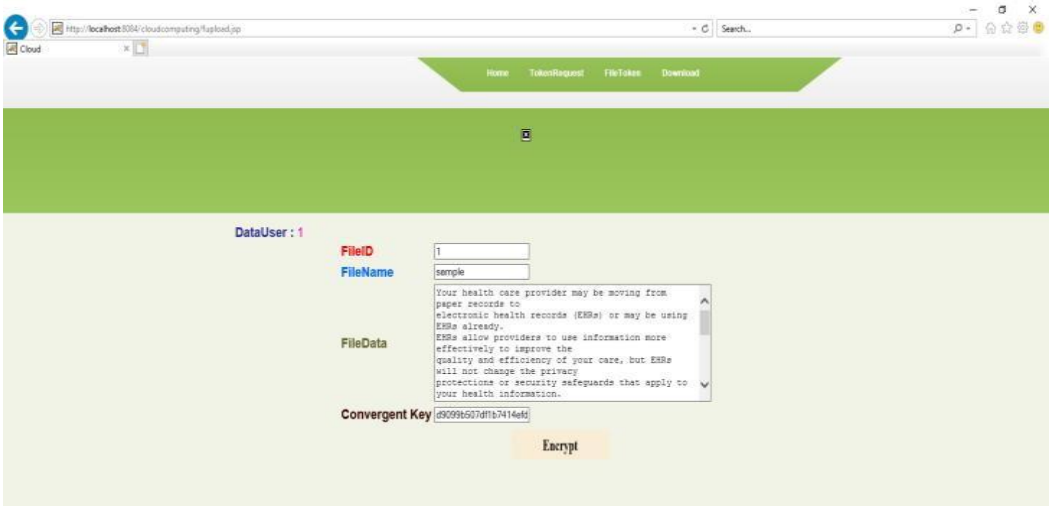


Figure 8.10 File upload slice encryption-1

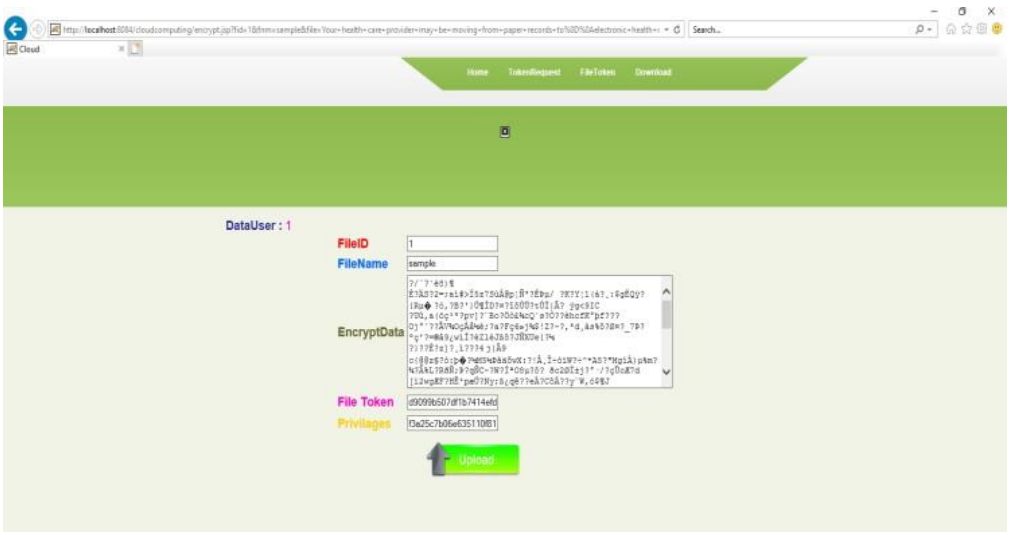


Figure 8.11 File upload slice encryption-2

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124163

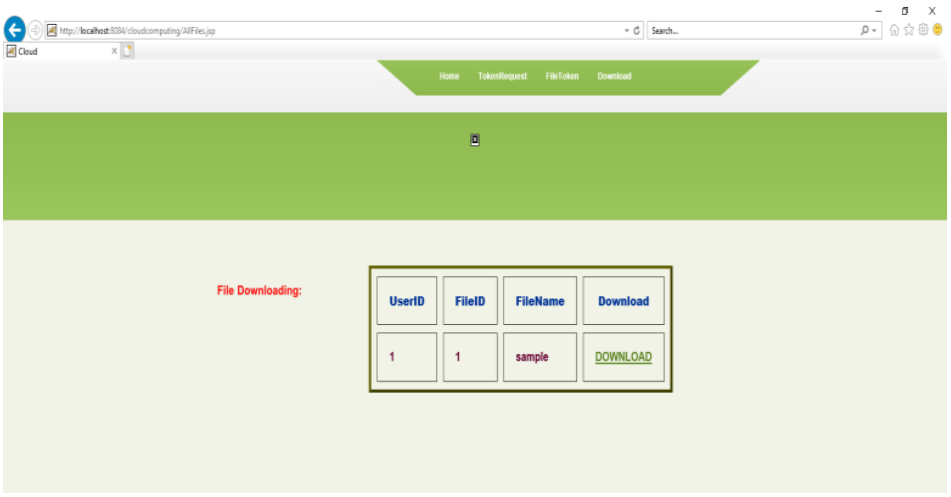


Figure 8.12 File download

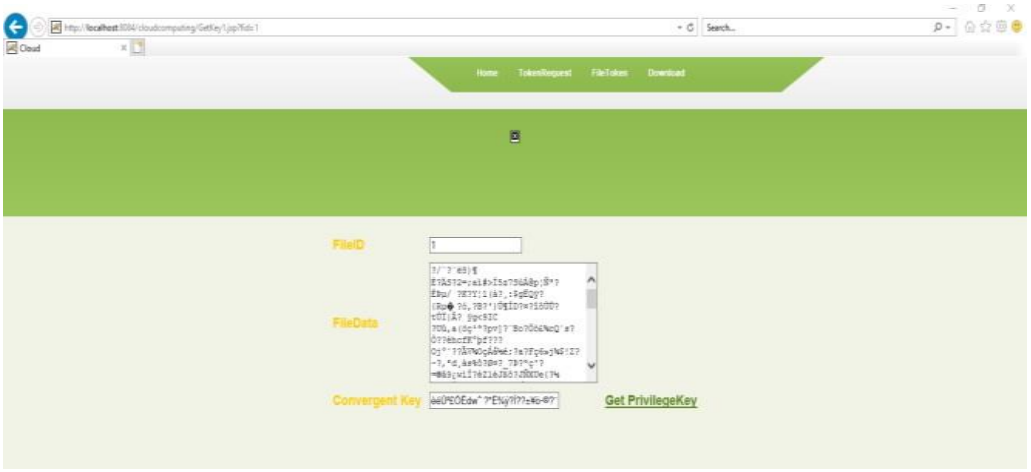


Figure 8.13 Decryption slice 1

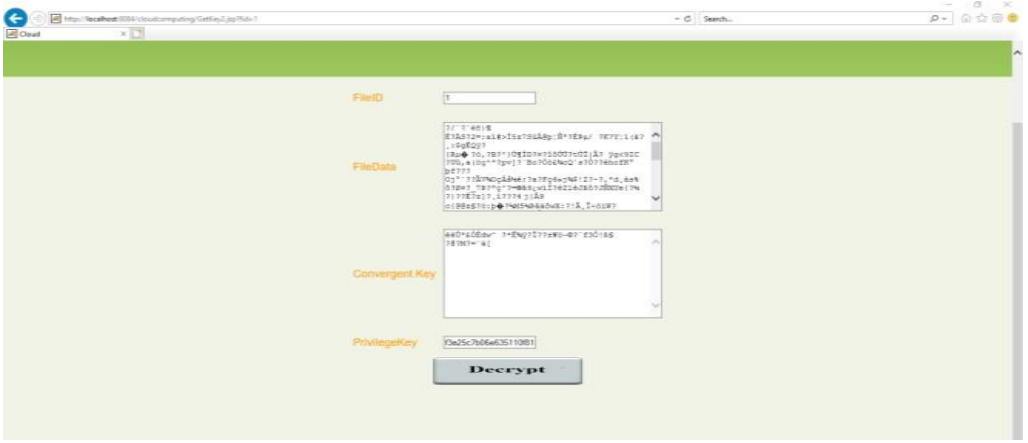


Figure 8.14 Decryption slice 2

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124163

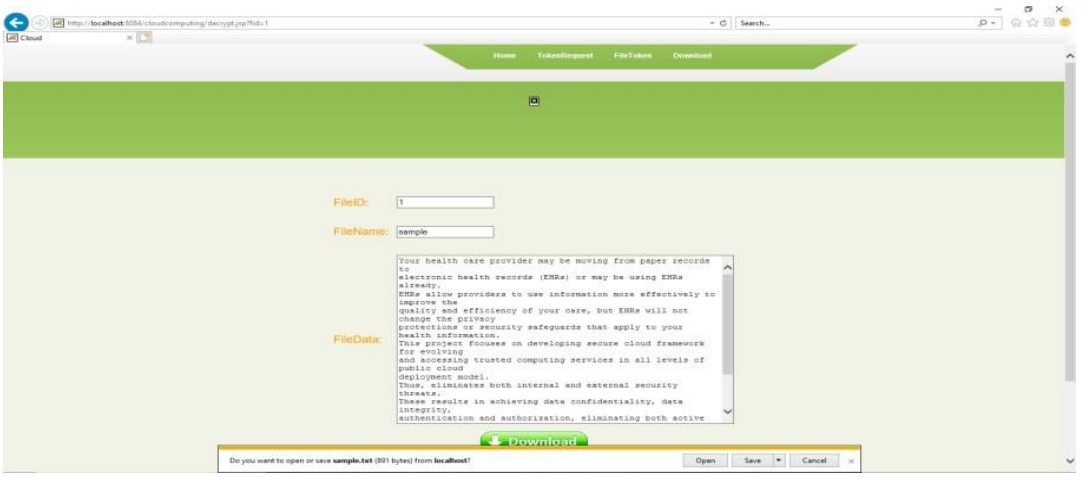


Figure 8.15 After download

X CONCLUSION

- By achieving data confidentiality, data integrity, authentication, and permission, the cloud network environment is free from active and passive threats.
- To create a secure cloud infrastructure that allows users to access reliable computing and storage services at all public cloud deployment model tiers.

XI FUTURE ENHANCEMENT

It doesn't include any security issues that might come up during the actual application of the current concept. Also, it improves national security. Deduplicating the data helps conserve memory, giving us access to enough of it. It grants permission to private companies and safeguards the privacy of sensitive information.

REFERENCES

[1] Kshetri, N., & Voas, J. (2018). Fog computing and its role in the internet of things and healthcare. Communications of the ACM, 61(5), 50-56.
[2] Alsaiari, R. A., Hussain, M., & Khan, S. U. (2019). Fog computing for healthcare: A review and future directions. Journal of Medical Systems, 43(3), 1-20.
[3] Alharthi, S., et al. (2019). Fog computing-based security framework for the internet of things in healthcare. Sensors, 19(5), 1175.
[4] Gondal, I., & Khattak, A. M. (2018). A secure fog-based healthcare monitoring system for smart cities. IEEE Access, 6, 54739-54748.
[5] Yang, K., & Li, C. (2019). A fog computing- based healthcare monitoring system using deep learning. Journal of Medical Systems, 43(4), 1- 11.
[6] Saberi, M., et al. (2019). A survey on fog computing: Concepts, applications, and issues. Internet of Things, 100222.
[7] Li, C., et al. (2019). A secure fog computing- based framework for privacy-preserving healthcare monitoring systems. Future Generation Computer Systems, 95, 770-780.
[8] Tao, Y., et al. (2019). A fog computing-based privacy-preserving system for healthcare big data analysis. IEEE Access, 7, 166766-166775.
[9] Wu, D., et al. (2018). A secure fog computing framework for privacy-preserving healthcare data processing. IEEE Access, 6, 58102-58111.
[10] Li, S., et al. (2019). A privacy-preserving and secure fog computing-based healthcare monitoring system. Future Generation Computer Systems, 101, 118-130.